worteks

make IT work, make IT free

LDAP TOOL BOX
SELF SERVICE PASSWORD

AFUP Lyon – 22 avril 2021

Présentation

Présentation

Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

LemonLDAP::NG
LDAP Tool Box
LDAP Synchronization Connector
FusionIAM
W'Sweet

KPTN
DonJon Legacy
Improcité

Worteks (\vɔʁ.tɛks\)

Worteks
make IT work, make IT free

Services

Infrastructures complexes et hétérogènes, cloud, messagerie, authentification, sécurité

- Étude, audit et conseil
- Expertise technique
- Support technique
- Formations
- R&D

Édition

V'Sweet — Portail applicatif et collaboratif

V'Opla — Plateforme collaborative mutualisée de développement

FUSION IAM — Gestion des identités et des accès

Partenaires

Collabora Online

BlueMind

redhat.
READY
BUSINESS PARTNER

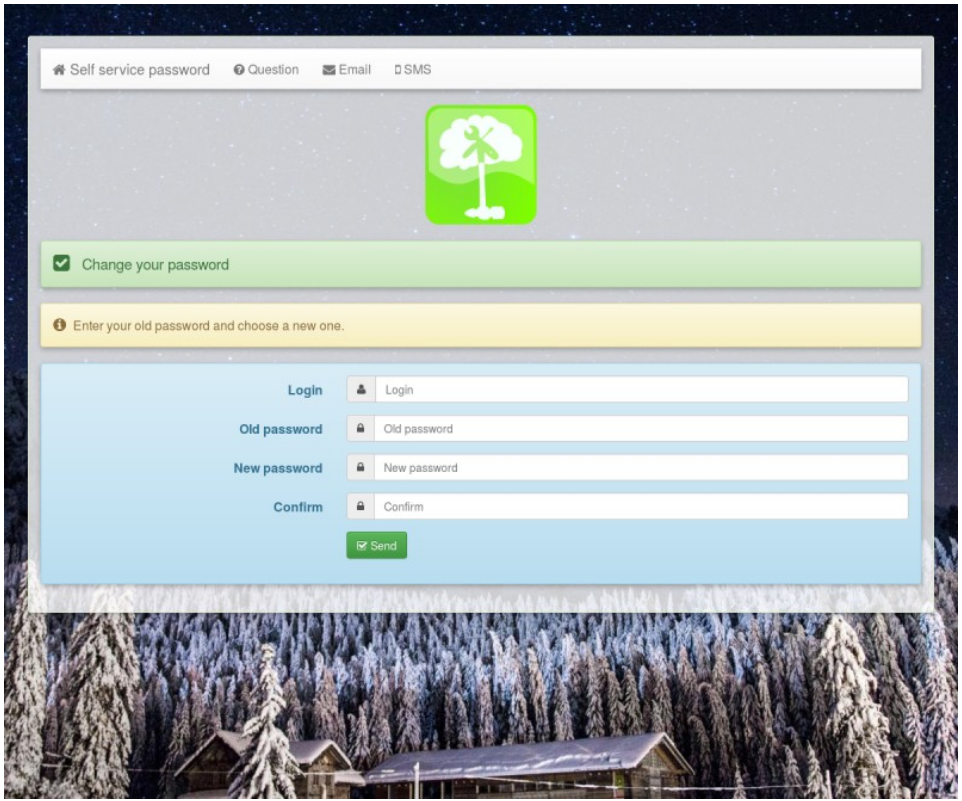
Le logiciel LTB Self Service Password

Le projet LDAP Tool Box

- Projet libre créé en 2009
- Regroupement d'outils dédiés à la gestion des annuaires LDAP
- Au début principalement des paquets OpenLDAP et des scripts de supervision
- Licence GPL

Self Service Password

- Interface de changement et réinitialisation de mot de passe dans un annuaire LDAP
- Compatible Active Directory et autres annuaires LDAPv3
- Réinitialisation par mail, SMS, questions/réponses
- Prehook/Posthook
- API REST



Historique

- Au début :
  - Premier commit le 16 juin 2009
  - Version 0.1 publiée le 20 juin 2009
  - Juste une page permettant de changer son mot de passe
- Aujourd'hui :
  - Version 1.4 publiée le 20 avril 2021
  - Traduit en 27 langues
  - Changement et réinitialisation de mot de passe, réinitialisation de clé SSH
  - Utilisation de Composer, Smarty, phpunit, PHPMailer, Bootsrap…

Pourquoi le choix de PHP (en 2009)

- Les avantages :
  - Langage disponible sur de nombreux serveurs, donc installation simplifiée
  - Connu par de nombreux développeurs, qui pourront donc plus facilement contribuer
- Les inconvénients :
  - Bibilothèque LDAP très sommaire (par rapport par exemple à Perl)

Quelques étapes

- 2009 : Version 0.1 :
  - 3 fichiers PHP : un fichier de configuration, un fichier de langues, un fichier contenant tout le reste du code
- 2016 : Version 1.0 :
  - Passage à bootsrap
  - Tests unitaires
  - Utilisation de PHPMailer
- 2021 : Version 1.4 :
  - Utilisation de Composer
  - Utilisation de Smarty

Le protocole LDAP

Opérations de base

- Authentification :
  - BIND
  - UNBIND
- Lecture :
  - SEARCH
  - COMPARE
- Écriture :
  - ADD
  - DELETE
  - MODIFY
  - MODIFYDN / MODRDN
- Autres :
  - ABANDON

Extensions du protocole

- Opérations étendues :
  - WHOAMI
  - MODIFYPASSWORD
  - ...
- Contrôles étendus :
  - PPOLICY
  - VLV
  - NOOP
  - PROXY AUTH
  - ...

Communication client/serveur

Client LDAP

Connexion TCP

Authentification (BIND)

Réponse BIND

Recherche (SEARCH)

Réponse SEARCH (+entrées)

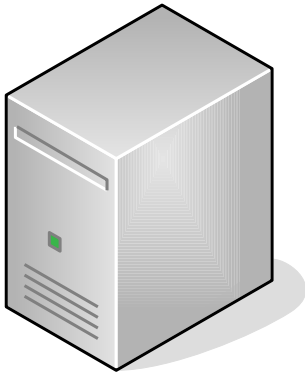
Authentification (BIND)

Réponse BIND

Modification (MODIFY)

Réponse MODIFY

Déconnexion (UNBIND)



Annuaire LDAP

Structure d'une entrée

RDN — Branche

DN: `uid=coudot,ou=users,dc=example,dc=com`

Attributs

```
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Clément OUDOT
sn: OUDOT
givenName: Clément
mail: clement.oudot@worteks.com
mail: cleoud@worteks.com
mobile: +33 6 99 66 51 31
uid: coudot
createTimestamp: 20161213142321Z
creatorsName: cn=admin,dc=example,dc=com
entryCSN: 20170901154823.930979Z#000000#001#000000
entryDN: uid=coudot,ou=users,dc=example,dc=com
entryUUID: 7180231a-558b-1036-86df-3f7f4c003ed8
```

Classes d'objets

Attributs opérationnels

Parler LDAP avec PHP

Connexion

```
# Connect to LDAP
$ldap = ldap_connect($ldap_url);
ldap_set_option($ldap, LDAP_OPT_PROTOCOL_VERSION, 3);
ldap_set_option($ldap, LDAP_OPT_REFERRALS, 0);
```

Authentification

```
# Bind
if ( isset($ldap_binddn) && isset($ldap_bindpw) ) {
    $bind = ldap_bind($ldap, $ldap_binddn, $ldap_bindpw);
} else {
    $bind = ldap_bind($ldap);
}
```

Modification du mot de passe

```
# Replace userPassword
$userdata["userPassword"] = $password;
ldap_mod_replace($ldap, $dn, $userdata);
$error_code = ldap_errno($ldap);
$error_msg = ldap_error($ldap);
```

Là où les ennuis commencent...

- Connexion sécurisée (LDAPS ou LDAP + startTLS)
- Rechercher l'utilisateur à partir de son identifiant pour retrouver son DN
- Gestion du mot de passe Active Directory différente des autres annuaires LDAP
- Enregistrement et recherche des questions/réponses dans l'annuaire
- Opérations et contrôles étendus

Usage avancé

Opération étendue PASSWORD MODIFY

- Fonction ldap_exop_passwd disponible depuis PHP 7.2

```
$exop_passwd = ldap_exop_passwd($ldap, $dn, $oldpassword, $password);
$error_code = ldap_errno($ldap);
$error_msg = ldap_error($ldap);
```

Contrôle étendu PASSWORD POLICY

- Fonction ldap_mod_replace_ext disponible depuis PHP 7.3

```
$ppolicy_replace = ldap_mod_replace_ext($ldap, $dn, $userdata, [['oid' =>
LDAP_CONTROL_PASSWORDPOLICYREQUEST]]);

if (ldap_parse_result($ldap, $ppolicy_replace, $error_code, $matcheddn, $error_msg, $referrals, $ctrls))
{
        if (isset($ctrls[LDAP_CONTROL_PASSWORDPOLICYRESPONSE])) {
            $value = $ctrls[LDAP_CONTROL_PASSWORDPOLICYRESPONSE]['value'];
            if (isset($value['error'])) {
                $ppolicy_error_code = $value['error'];
            }
        }
```

worteks

make IT work, make IT free

MERCI

info@worteks.com

@worteks_com

linkedin.com/company/worteks